

Решение задачи о назначении ролей в ролевой модели безопасности методами линейного программирования

С.В. Усов
raintower@mail.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация

Рассматриваются две постановки задачи о назначении ролей в рамках ролевой политики разграничения доступа. В рамках задачи требуется назначить набор ролей пользователю таким образом, чтобы его потребности в полномочиях были удовлетворены, при этом ущерб, наносимый информационной системе, был бы минимальным. В первой задаче минимизируется ущерб, возникающий вследствие возможной компроментации ролей этого пользователя. Во второй задаче минимизируется ущерб от использования субъектом полученного в рамках назначенных ролей излишнего полномочия. Для каждой задачи предлагается формализация в виде задачи линейного программирования и метод решения.

1 Проблема утечки полномочий в иерархической ролевой модели безопасности

Ролевая модель разграничения доступа [1] базируется на идее разбиения множества субъектов на классы, называемые ролями, такие, что каждой роли приписывается определенный набор привилегий (или полномочий). Каждая привилегия, если подходить с точки зрения дискреционной политики безопасности, представляет собой предзаданный набор прав на определенные объекты. Пользователь получает соответствующий роли набор полномочий при авторизации на эту роль.

В ролевой модели безопасности определяются $R = \{r_1, \dots, r_n\}$ – множество всех ролей системы, и $P = \{p_1, \dots, p_m\}$ – множество всех привилегий системы. Каждой роли сопоставлен определенный набор привилегий. На множестве ролей вводится частичный порядок, тем самым задается иерархия, которую можно представить в виде ориентированного графа (ациклического). Если роль r находится в иерархии выше роли r' , то есть $r > r'$, то она обладает всеми привилегиями, которыми обладает роль r' . Иерархию будем представлять ориентированным деревом, в котором нелистовым вершинам соответствуют вспомогательные роли, листовым – роли конечных пользователей. Множество полномочий, соответствующих роли r , будем обозначать $r.p$.

Проблема утечки прав доступа – ключевая проблема в направлении изучения моделей безопасности компьютерных систем. В случае ролевой модели ее можно интерпретировать как проблему утечки полномочий или же ролей. В [2] предложена методика оценки вероятностей утечки полномочий.

Эта методика применяется в условиях трех предположений о модели злоумышленника в условиях ролевой политики безопасности. Перечисленные ниже предположения используются в качестве аналога

Copyright © by the paper's authors. Copying permitted for private and academic purposes.

In: Sergey V. Belim, Nadezda F. Bogachenko (eds.): Proceedings of the Workshop on Data, Modeling and Security 2018 (DMS-2018), Omsk, Russia, October 2018, published at <http://ceur-ws.org>

экспертных оценок в методе анализа иерархий, оценивается риск утечки полномочий.

1. Чем больше полномочий содержит роль, тем выше вероятность атаки на нее.
2. Чем чаще встречается полномочие, тем выше вероятность его утечки.
3. Чем выше роль в иерархии, тем выше вероятность атаки на нее.

Далее, в [3] была предложена методика оценки ущерба вследствие захвата злоумышленником той или иной роли в компьютерной системе с ролевым разделением прав доступа при условии, что возможно подсчитать либо оценить ущерб, возникающий по причине утечки каждого из полномочий. В случае невозможности оценки последнего ущерба предложено использовать формулу оценки относительного ущерба, также эксплуатирующую предположения того же характера, что и выше. Вот эти предположения:

1. Чем реже встречается привилегия в иерархии ролей, тем выше ущерб от ее утечки.
2. Чем реже встречается привилегия среди листовых ролей (которые назначаются конечным пользователям), тем выше ущерб от ее утечки, причем зависимость носит экспоненциальный характер.

2 Задача о назначении ролей. Фактор утечки ролей

Данная работа будет посвящена решению следующей задачи:

Дана компьютерная система с ролевым разграничением доступа. Множества ролей и привилегий, а также иерархия ролей заданы. Для каждого субъекта определен необходимый и достаточный набор полномочий, который ему потребуется в рамках функционирования в компьютерной системе. Также считаем известным ущерб от нарушения безопасности системы по причине утечки роли.

Требуется определить, какой набор ролей сопоставить каждому субъекту, чтобы его потребности в полномочиях были удовлетворены, а связанный с утечкой этих ролей ущерб был бы наименьшим.

В рамках данной задачи фактически требуется минимизировать ущерб, который может быть нанесен информационной системе в результате успешного перехвата ролей, назначенных субъекту, со стороны третьих лиц.

Поскольку задача носит оптимизационный характер, сформулируем ее в терминах линейного программирования.

Пусть для рассматриваемого субъекта задан вектор необходимых полномочий $b = (b_1, \dots, b_m)$, $b_i \in \{0, 1\}$, $i = 1 \dots m$. Здесь полномочию p_i отвечает значение $b_i = 1$, если оно является необходимым для субъекта, и значение $b_i = 0$ в противном случае. Множество необходимых субъекту s полномочий обозначим через P_s .

Наборы полномочий, соответствующие ролям в рамках данной модели оформим в виде матрицы A размера $m \times n$, в которой каждому полномочию соответствует строка, каждой роли – столбец, и $a_{ij} = 1$ только если роль r_j наделена полномочием p_i , в противном случае $a_{ij} = 0$.

Считаем, что набору ролей сопоставлен вектор ущерба $d = (d_1, \dots, d_n)$, где $d_j \geq 0$ – оценка ущерба, который наносится системе при утечке роли r_j , $j = 1 \dots n$.

Наконец, решение будем искать в виде вектора назначений $x = (x_1, \dots, x_n)$, $x_j \in \{0, 1\}$, $j = 1 \dots n$. Здесь $x_j = 1$ означает, что субъект наделяется ролью r_j , а $x_j = 0$ в случае, когда субъект ролью r_j не наделяется.

В этом случае целевую функцию задачи линейного программирования можно записать в виде

$$f(x) = \sum_{j=1}^n d_j x_j \rightarrow \min,$$

а линейные ограничения задачи окажутся следующие:

$$\begin{aligned} \sum_{j=1}^n a_{ij} x_j &\geq b_i, \quad i = 1 \dots m, \\ x_j &\in \{0, 1\}, \quad j = 1 \dots n. \end{aligned}$$

Данная задача относится к классу задач целочисленного программирования и легко приводится к канонической форме (задаче Риды). Таким образом, задача может быть решена симплекс-методом с использованием метода отсечений [4].

Теорема 1. *Задача о назначении ролей в условиях известного ущерба от утечки роли является разрешимой если и только если $P_s \subseteq \bigcup_j r_j.p$.*

Доказательство. Если задача разрешима, рассмотрим ее оптимальное решение x^* и соответствующее ему подмножество ролей R^* ($r_j \in R^* \iff x_j = 1$). Получаем цепочку включений

$$P_s \subseteq \bigcup_{r_j \in R^*} r_j \cdot p = \bigcup_{x_j=1} r_j \cdot p \subseteq \bigcup_j r_j \cdot p,$$

в которой первое включение следует из того, что оптимальное решение является допустимым.

Обратно, если $P_s \subseteq \bigcup_j r_j \cdot p$, то можно рассмотреть решение $x = (1, \dots, 1)$, то есть вектор, состоящий из всех единиц (субъект наделяется всеми ролями системы). Такое решение, как несложно проверить подстановкой, является допустимым в рамках данной задачи линейного программирования, то есть область допустимых решений задачи не пуста. С другой стороны, целевая функция ограничена снизу, поскольку $d_j \geq 0$, $x_j \geq 0$. Непустота области допустимых решений вкупе с ограниченностью целевой функции на ней является необходимым и достаточным условием разрешимости задачи линейного программирования. Впрочем, достаточно было бы указать, что в рамках данной целочисленной задачи непустая область допустимых решений ограничена булеаном, поэтому решение задачи можно свести к перебору 2^n возможных значений вектора x и выбору удовлетворяющего системе линейных ограничений вектора, на котором достигается наименьшее значение целевой функции. ■

Рассмотрим пример решения поставленной задачи на примере иерархии ролей T^1 , представленной на рис. 1.

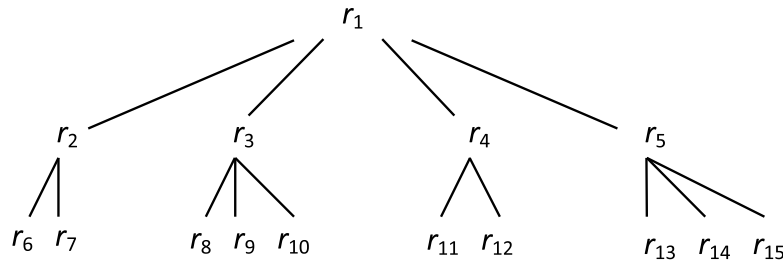


Рис. 1: Ролевое дерево T^1

Пусть используется нестрогий таксономический подход к распределению полномочий, и полномочия листовых ролей имеют следующие значения: $r_6 \cdot p = \{p_1, p_2, p_3\}$, $r_7 \cdot p = \{p_2, p_4\}$, $r_8 \cdot p = \{p_3, p_4, p_5\}$, $r_9 \cdot p = \{p_3, p_5\}$, $r_{10} \cdot p = \{p_2, p_4\}$, $r_{11} \cdot p = \{p_2, p_5\}$, $r_{12} \cdot p = \{p_1, p_4, p_5\}$, $r_{13} \cdot p = \{p_3, p_5\}$, $r_{14} \cdot p = \{p_1, p_2, p_5\}$, $r_{15} \cdot p = \{p_5\}$.

В работе [3] были посчитаны относительные оценки ущерба от успешной атаки на каждую из ролей. Мы воспользуемся этими оценками в нашем примере. Считая, что субъекту будет назначен набор из числа листовых ролей, выпишем вектор ущерба согласно [3]:

$$d = (0,072; 0,057; 0,066; 0,052; 0,057; 0,051; 0,069; 0,052; 0,067; 0,039).$$

Поскольку у листовых ролей индекс принимает значения от 6 до 15, при построении модели в векторах x и d , а также в использующих их формулах, индекс j будет пробегать тот же диапазон значений.

Матрица системы A , построенная на основе иерархии ролей, будет иметь следующий вид:

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Пусть субъекту для работы в системе необходимы полномочия $P_s = \{p_1, p_3, p_4\}$, то есть вектор необходимых полномочий имеет вид $b = (1, 0, 1, 1, 0)$.

Целевая функция задачи и система линейных ограничений примут следующий вид:

$$f(x) = 0,072x_6 + 0,057x_7 + 0,066x_8 + 0,052x_9 + 0,057x_{10} + 0,051x_{11} + 0,069x_{12} + 0,052x_{13} + 0,067x_{14} + 0,039x_{15} \rightarrow \min,$$

$$x_6 + x_{12} + x_{14} \geq 1,$$

$$\begin{aligned}
x_6 + x_7 + x_{10} + x_{11} + x_{14} &\geq 0, \\
x_6 + x_8 + x_9 + x_{13} &\geq 1, \\
x_7 + x_8 + x_{10} + x_{12} &\geq 1, \\
x_8 + x_9 + x_{11} + x_{12} + x_{13} + x_{14} + x_{15} &\geq 0, \\
x_j &\in \{0, 1\}, \quad j = 6 \dots 15.
\end{aligned}$$

Решая задачу любым из предложенных способов (симплекс-методом или перебором решений), получаем наименьшую оценку ущерба 0,121 при назначении субъекту ролей r_{12} и r_{13} .

3 Задача о назначении ролей. Фактор утечки полномочий

Рассмотрим следующую задачу:

Дана компьютерная система с ролевым разграничением доступа. Множества ролей и привилегий, а также иерархия ролей заданы (будем считать, что каждое полномочие приписано хотя бы одной роли). Для каждого субъекта определен необходимый и достаточный набор полномочий, который ему потребуется в рамках функционирования в компьютерной системе. Также считаем известным ущерб от нарушения безопасности системы по причине утечки полномочия.

Требуется определить, какой набор ролей сопоставить каждому субъекту, чтобы его потребности в полномочиях были удовлетворены, а ущерб связанный с утечкой полномочий, полученных субъектом, но не являющихся необходимыми для его работы в системе, был бы наименьшим.

В данном случае требуется минимизировать ущерб информационной системе, который может произойти за счет того, что субъект, которому назначаются роли, воспользуется входящим в этот набор ролей правом доступа, которое не требуется для непосредственного исполнения его обязанностей. Как видно, данная задача по цели существенно отличается от рассмотренной ранее.

Данная задача также оптимизационная, и допускает формулировку в терминах линейного программирования.

Как и ранее, считаем, что определены:

- вектор необходимых полномочий субъекта $b = (b_1, \dots, b_m)$, $b_i \in \{0, 1\}$, $i = 1 \dots m$,
- множество P_s необходимых субъекту s полномочий,
- матрица A размера $m \times n$ наборов полномочий,

Считаем, что набору полномочий сопоставлен вектор ущерба $d = (d_1, \dots, d_m)$, где $d_i \geq 0$ – оценка ущерба, который наносится системе при утечке полномочия p_i , $i = 1 \dots m$.

Наконец, решение будем искать в виде вектора назначений $x = (x_1, \dots, x_n)$, $x_j \in \{0, 1\}$, $j = 1 \dots n$. Здесь $x_j = 1$ означает, что субъект наделяется ролью r_j , а $x_j = 0$ в случае, когда субъект ролью r_j не наделяется.

Также введем дополнительный вектор назначенных полномочий $y = (y_1 \dots y_m)$, $y_i \in \{0, 1\}$, $i = 1 \dots m$. Здесь $y_i = 1$ означает, что субъект в результате назначения ему ролей согласно вектору назначений x получает полномочие p_i , а $y_i = 0$ в случае, когда субъект полномочие p_i не наделяется.

В этом случае целевую функцию задачи линейного программирования можно записать в виде

$$f(x) = \sum_{i=1}^m d_i(y_i - b_i) \rightarrow \min,$$

а линейные ограничения задачи окажутся следующие:

$$\begin{aligned}
\sum_{j=1}^n a_{ij}x_j &\geq y_i \geq b_i, \quad i = 1 \dots m, \\
x_j &\in \{0, 1\}, \quad j = 1 \dots n, \\
y_i &\in \{0, 1\}, \quad i = 1 \dots m.
\end{aligned}$$

Данная задача, как и предыдущая, относится к классу задач целочисленного программирования и легко приводится к канонической форме (задаче Риды). Таким образом, и эта задача может быть решена симплекс-методом с использованием метода отсечений.

Теорема 2. *Задача о назначении ролей в условиях известного ущерба от утечки полномочия является разрешимой если и только если $P_s \subseteq \bigcup_j r_j.p$.*

Доказательство. Если задача разрешима, рассмотрим ее оптимальное решение (x^*, y^*) и соответствующее ему подмножество ролей R^* ($r_j \in R^* \iff x_j = 1$). Получаем цепочку включений

$$P_s \subseteq \bigcup_{r_j \in R^*} r_j.p = \bigcup_{x_j=1} r_j.p \subseteq \bigcup_j r_j.p,$$

в которой первое включение следует из того, что оптимальное решение является допустимым.

Обратно, если $P_s \subseteq \bigcup_j r_j.p$, то можно рассмотреть решение $(x, y) = (1, \dots, 1)$, то есть вектор, состоящий из всех единиц (субъект наделяется всеми ролями системы, а значит и всеми полномочиями системы). Такое решение, как несложно проверить подстановкой, является допустимым в рамках данной задачи линейного программирования, то есть область допустимых решений задачи не пуста. С другой стороны, целевая функция ограничена снизу, поскольку $d_i \geq 0$, $y_i \geq 0$. Непустота области допустимых решений вкупе с ограниченностью целевой функции на ней является необходимым и достаточным условием разрешимости задачи линейного программирования. С другой стороны, как и при доказательстве теоремы 1, достаточно сослаться на конечность непустого множества допустимых решений, что позволяет решить задачу перебором. ■

Рассмотрим пример решения поставленной задачи на основе представленной на рис. 1 иерархии с нестрогим таксономическим распределением полномочий.

Оценку относительного ущерба от утечки полномочий возьмем из работы [2].

$$d = (0, 14; 0, 23; 0, 16; 0, 17; 0, 30).$$

Матрица системы A , построенная на основе иерархии ролей, будет иметь тот же вид, что и ранее.

Пусть субъекту для работы в системе необходимы полномочия $P_s = \{p_1, p_3, p_4\}$, то есть вектор необходимых полномочий имеет вид $b = (1, 0, 1, 1, 0)$.

Запишем целевую функцию задачи и систему линейных ограничений:

$$f(x) = 0,14y_1 + 0,23y_2 + 0,16y_3 + 0,17y_4 + 0,30y_5 \rightarrow \min,$$

$$x_6 + x_{12} + x_{14} \geq y_1 \geq 1,$$

$$x_6 + x_7 + x_{10} + x_{11} + x_{14} \geq y_2 \geq 0,$$

$$x_6 + x_8 + x_9 + x_{13} \geq y_3 \geq 1,$$

$$x_7 + x_8 + x_{10} + x_{12} \geq y_4 \geq 1,$$

$$x_8 + x_9 + x_{11} + x_{12} + x_{13} + x_{14} + x_{15} \geq y_5 \geq 0,$$

$$x_j \in \{0, 1\}, \quad j = 6 \dots 15,$$

$$y_i \in \{0, 1\}, \quad i = 1 \dots m.$$

Решая задачу любым из предложенных способов (симплекс-методом или перебором решений), получаем наименьшую оценку ущерба 0,23 при назначении субъекту ролей r_6 и r_7 .

Список литературы

- [1] D.F. Ferraiolo, D.R. Kuhn. Role-Based Access Control. *15th National Computer Security Conference*, 554–563, October 1992.
- [2] S.V. Belim, N.F. Bogachenko. Using a Hierarchy Analysis Method to Assess Permission Leakage Risks in Systems with a Role Based Access Control. *Information and Control Systems*, 6:67–72, 2013 (In Russian).
- [3] N.F. Bogachenko, S.V. Usov. On the estimation of the damage from the leakage of permissions in a role-based security model. *CEUR Workshop Proceedings*, Vol. 1965, 2017.

- [4] V. Klee. How good is the simplex algorithm? *Inequalities III, Proceedings of the Third Symposium on Inequalities held at the University of California*, Los Angeles, Calif., September 1–9, 1969, dedicated to the memory of Theodore S. Motzkin. New York-London: Academic Press, 1972, P. 159–175.

Solution of the Problem of Assigning Roles in the Role-Based Access Control Model Using Linear Programming Methods

Sergey S. Usov

Two formulations of the role assignment problem within the role-based access control policy are considered. As part of the problem, it is required to assign a set of roles to the user in such a way that his needs for permissions are met, while the damage caused to the information system would be minimal. In the first problem, the damage arising due to the possible leakage of the roles of the user is minimized. In the second problem, the damage from the use of excessive permission received by the subject is minimized. For each problem, formalization in the form of a linear programming problem is proposed and a solution method is given.